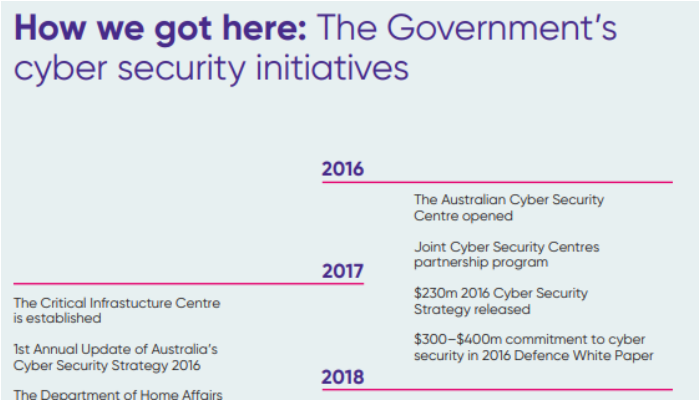
Strengthening Australia's cyber security regulations and incentives

Introduction

- I make this submission to "Strengthening Australia's cyber security regulations and incentives", as an independent Australian technologist (over two decades purely in Australia).
- As you would be aware, technology governance is vastly different and more complex than business governance in general, though it encompasses the latter. You will see clear examples below, of how this confusion is unhelpful. Business/Corporate Governance is only a small subset.
- I have no current or past ties to any of the influencing big-tech/big-media – I have no interests in such large corporations.
- As will be detailed below, this is not the first time Australian Governments have asked many of these questions.
- I have also participated in similar open/closed submissions for nearly two decades.

Pre-existing similar initiatives to this discussion paper

- This discussion paper describes "How we got here" as historically commencing in 2016;



- I would like to acknowledge that:
    - Collaboration has existed for over two decades with members of the Australian Cyber industry (including Cyber Security).
    - The topics had traditionally been bi-partisan or more accurately partisan-free – if there is such a thing.
    - The Cyber and Cyber Security industries have been around for decades in Australia.
    - The decline of the independent (home-grown) Cyber producers of Australia, including Cyber Security, is more evident in the last decade, and more so than ever before in Australian history. OECD data has shown that the GVA (contributions to GDP) of ICT has been in decline since 2001 in Australia, when it was increasing in other nations. A more recent and questionable view is that ICT has flourished over the past few years, however the organisations that have emerged after the ICT industry decline are largely adopters not producers in Australia. To illustrate that as an example, using an "AI" programming framework is too often mistaken as having an AI that is commercially/objectively viable. OECD data also correlates with Employment Data trends, since 2001. This indicates decline in the employment of

more senior and higher skilled workers (effectively cycling seniors out as they achieve seniority). This has been assisted by various government policies that directly target ICT and other workers negatively. This has resulted in a high-risk knowledge-gap in the existing industry, and this is likely being exploited.
    - Both women and men played integral parts in building the industry and such strategies prior to 2016.
    - There should be no separation between technical and non-technical skills. A person cannot have knowledge in the **technical** without knowledge of the non-technical & mastered both. In-fact its deficiencies in not being across the spectrum that often get exploited. E.g. high risk organisations include; those that lean too far towards non-technical people working and leading in technical fields.
- I would like to point out that many of the questions and topics, in this discussion paper, are not new to Australian Government. In fact, many had been answered prior to 2016 – they are still the same challenges and, in many cases, the same answers. For example, within the "Cyber White Paper" of 2011:
    - It included a broad range of various views and submissions including those of various federal and state departments.
    - More info is found here: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/1087528%22
    - Records and submissions have been removed from public availability, such as; in the removal of www.cyberwhitepaper.dpmc.gov.au
    - There should be no sensitivity surrounding the removal of those submissions, most of them are publicly made available by their authors anyway.
    - To illustrate similarities and currency of the previous enquiry; below is a summary of the topics/questions raised in the Cyber White Paper from 2011 – which are quite broad. These are topics from over a decade ago, and they cut to the heart of the topics raised in this discussion paper today.

Cyber White Paper 2011 Questions

Topic	Question from 2011
Digital citizenship in a networked society	How can we promote a concept of digital citizenship, reach agreement on acceptable online behaviour and encourage people to assume greater responsibility for that behaviour?
	How can governments, the private sector, the NFP sector and the broader Australian community work together to promote responsible and accountable digital citizenship and reduce harassing and malicious online behaviour?
	How can we help carers and parents to appropriately supervise young people and minimise these online risks?
	How can we promote social responsibility and encourage young people to protect themselves and each other by speaking out against cyberbullying?
	How can the owners of social networking sites be more engaged in meeting community expectations that their platforms will not be used for abusive or illegal activities?
	What new and innovative opportunities do social networking tools provide to improve the social well-being of Australians?
	How can NFPs ensure the security of online fundraising activities conducted through social networking sites?
	How can governments improve citizens' and businesses' trust that their private data will be secured and only used for agreed purposes?
Protecting and promoting Australia's digital economy	How can small business awareness of commercial online opportunities be balanced with awareness of potential online risks and mitigation strategies?
	How can governments, industry, NFPs and consumer groups boost consumers' confidence to engage in e-commerce?
	How can governments and the private sector continue to build and maintain confidence in the digital economy while also raising awareness among consumers and small businesses of the nature of cyber threats?
	How can we improve and encourage the reporting of data breaches in Australia?

	How can e-businesses more effectively work together to develop a self regulatory feedback system that provides a way of sharing their experiences with other online traders?
	What does the Australian public expect from policing and consumer protection agencies in relation to preventing and investigating cyber crimes?
	What options are there for increasing consumers' trust in conducting business online?
	How can consumers be encouraged to take more responsibility to protect their information?
	What are the options for broadening industry's efforts to provide customers with a greater level of trust and confidence in the security and privacy of their online transactions?
	What information would help consumers and small businesses better protect themselves and enhance their trust and confidence online?
	What do consumers and small businesses expect from their Internet Service Providers (ISPs), software and hardware providers and the government to assist them to maintain or enhance their confidence online?
	How can governments and industry work together to make Australia a difficult place for cyber criminals to target?
	What are the options for limiting the collective economic and societal costs of widespread individual security lapses?
	What role do individuals, businesses and, more specifically, ISPs and large online companies, have in limiting the collective harm compromised computers have on the Australian economy and to the broader well-being of the Australian community?
	How can Commonwealth and state and territory governments encourage victims to report incidences of cyber crime and scams and better assist them with support and advice?
	How can Commonwealth and state and territory governments obtain the information and data required to form a more precise assessment of the extent of the economic and social harm caused by cyber crime?
	How can government, ISPs, financial institutions and small businesses collaboratively create an environment where small businesses are empowered to operate in a safe and secure manner online?

Security and resilience in the online environment	How can the Commonwealth, states and territories and industry effectively communicate the interdependent nature of individual and national cyber security? How can the importance of individual behaviour be highlighted in creating a secure, trusted and resilient online environment for all Australians?
	How can citizens better protect themselves from cyber threats?
	Are individuals adequately aware of cyber threats and the steps they should take to protect themselves? If not, why not?
International partnerships and Internet governance	What model of Internet governance is in the best interests of all Australians?
	How can we get the right balance between Australia's social, economic and security needs when developing an Australian vision for the online environment?
	What sort of approach should be taken to developing agreements on behaviour in the online environment?
Investing in Australia's digital future	What strategies should be pursued by governments, industry and academia to ensure adequate levels of domestic expertise are available to maximise the opportunities of the digital economy and address risks to Australia's digital infrastructure?
	What new forms of government-industry cooperation and dialogue are required to ensure the Australian cyber skills base is developed to meet Australia's broader national interests?
	How can we ensure all sectors of the Australian community have the necessary skills and security awareness to optimise the benefits of the digital economy?
	Besides rolling out the NBN, what role does the government have in promoting opportunities for individuals and businesses to compete in the global information communications technology marketplace and to increase the attractiveness of Australia as a destination for digital investment?

What are the factors preventing the adoption of cyber security best practice in Australia?

- When we examine the available job ads in Australia, nearly all ICT job ads are in tech adoption (re-use of existing technologies) and not in tech creation (genuine exportable innovation). Where in the previous two decades it was the opposite.
- While I stress that trade and agreements may be important, it is still important to point out that the primary factor preventing the adoption of cyber security practices; is the decline of the independent, Australian self-origin, Cyber industry – over the last decade. Instead, the focus is given to large corporations (including banks, and telecommunications providers) and how those corporations *respond* to cyber security (*reactive*).
    - These organisations are largely adopters of cyber security and rarely mandate the necessary expertise across the spectrum, of technical and non-technical skills, to create next-generation cyber technologies and techniques.
    - The expertise still exists in Australia, there is no shortage of skills. We need to ask; what's happened to those skills?. Unusually and insensibly, the incentive to business is configured to reduce workforce costs instead – this appears to be a recent government strategy to limit inflation as the technology workforce replaces others over time (disinflation, see other mentions of this). Take note that the government itself uses Big-Consulting firms and labour hire workforces for Cyber, the impact of which is under public examination.
- The legislative framework does not assist in adequately protecting Australian technology IP:
    - This, amongst other reasons, leads to the fact that Australian Cyber orgs/workers would have to move their operations overseas, to sell back to Australia.
    - The Australian banking industry is also known to act against Australian technology organisations (not just blockchain or FinTech) with hostile techniques now known as "de-banking" – capitalising on confusion and regulation-transparency (lack thereof).
    - Organisations must be sufficiently funded so that to protect IP, and that is very rare given the strength of possible loopholes in existing IP protections.
- The concept of best practices is a tiny contributor to Cyber Security and the reduction of Cyber Security practices so that to form it into a Quality Assurance (tick the box, business governance) exercise would be devastating to the Australian economy – opening the doors to exploitation beyond what is already happening.

Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

- Big businesses have become acutely aware of the regulatory frameworks, and the impact of technologies. It should be made no-less-than a criminal offence if workers are coerced into participating in acts of "negative externalities" (deliberate or otherwise, where knowledge of the negative externality existed – as with all criminal conduct; *mens rea*). That includes direct criminal charges against managers and-also directors. Anything less will mean that there will never be a level playing field in business in Australia. Most technologists within organisations have adequate skills and training to identify and report issues clearly. Technologists are likely to report, the impact, in advance to their superiors. There is no true excuse for technology glitches. The formation of such a criminal act should supersede existing allowances in other regulatory frameworks so that to deter the creation of loopholes in those frameworks by using technology as an excuse.

    - Treating this coercion as a crime, rather than a compliance issue, will incentivise boards to:
        - Build and configure focussed budgets, very quickly.
        - Build pathways for technical staff to step into leadership.
        - Mandate the building of governance frameworks that are also lead by qualified (highly-technically experienced) staff.
- Online technologies have now existed for over two decades in Australia. The public expects that corporations should be held to account with all technology issues and glitches -- regardless. The public tolerance has been reduced especially due to the behaviours of the banking and telecommunications industries in Australia (and-also multi-nationals). Accountability is the cost of doing business.
- Similarly, to the above; trust in supply-chains such as Big-Tech, Big-Consulting, Big-Media is low. These have consistently shown to exploit their position when it comes to Cyber or Cyber Security in various ways. Examples include, and are not limited to;
    - Big-Tech with unsuitable offerings having security holes.
    - Big-Consulting with large, lucrative, contracts to customise Big-Tech.
    - Big-Media with issues in; advertising, data, privacy.
- It is already extremely well established that information symmetries are exploitative by supply-chains. Even if corporations, big-tech, big-consulting, big-media are obligated to disclose issues, they typically don't. This means self-regulation is also useless and far too weak.
    - Similarly, it is nearly impossible for businesses or consumers to report issues with big-tech, big-consulting, big-media to current or future regulators – and have it actioned.
    - No single government organisation oversees the recording of business or consumer reports, and is also tasked to prosecute failures at the same time.
    - These big businesses are acutely aware they can silence reports using further technical issues also (e.g. complaint forms not working is an active strategy used).
    - These big businesses are acutely aware they can provide defective products without repercussion, and actively adjust their offerings to maintain that status quo.
    - These big businesses are acutely aware of confusions that could arise and be exploited.
- The debates about "negative externalities" and "information asymmetries" is likely driven by confusion around accountability and liability (and insurance). Corporations wants to point the blame at others, to create confusion, and also to get a free-ride with liabilities. Risk profiling is being used as a tool to confuse further. The existence of cyber security insurance at all is questionable.

What are the strengths and limitations of Australia's current regulatory framework for cyber security?

- We must continue with the status quo of requiring extra-jurisdictional large organisations to register and comply with Australian law, as recommended by various submissions to parliament in the Cyber White Paper 2011.
- The current framework is fragmented into various departments. While there are pockets of great cyber strategies, the existing departmental role-structures mean that there are no truly-unified efforts that could be effective. Great examples of failures include:

    - That it took over a decade to resolve security issues with SMS and spam calls with various telecommunications providers – something that otherwise is very simple to achieve. Till today, it is still not a unified effort.
        - This is likewise with Australian websites which is not resolved (but considerably more complex, yet a straightforward option). This is dissimilar to the block-list debates.
    - Another example is the hijacking of DNS by DNS and telecommunications providers so that customers cannot reasonably change providers. This problem continues to exist, yet it is a very well-known problem.
    - Another example is the recent outage by the Australian banks that used a common application network provider. This brought down several banks in Australia. That issue would not have been possible if the technology governance strategies of the previous decade where still in place by the banks. This issue is a direct result of being an adopter not a creator of technology as well as the de-skilling of the industry. I commend NAB for having designed their systems better than others.
    - There are in fact hundreds of unreported examples further to this.
- The current legislative frameworks are too soft. Public sentiment agrees they are too soft. It is likely that business will agree they are too soft. Society has reached a critical tipping point where there are enough technology workers, who understand the legislative failures, deeply and from experience.

How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

What is the best approach to strengthening corporate governance of cyber security risk? Why?

Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?

What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)? What technologies, sectors or types of data should be covered by a code under the Privacy to achieve the best cyber security outcomes?

Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security?

What other action should the Government consider, if any?

What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights consumers?

- Obviously as a general principle, we shouldn't regulate the possibilities and technologies, but regulate how they should-not be used, and in a strongly enforceable way.
- Current approaches to cyber security risk are complicated. They are not required if specific criminal offenses are created (see below). It is a futile exercise to even attempt to profile what I termed in 2008 as the "fluid-risk" that exists. These risks will change before such an exercise ends anyway.
- The current status quo of director personal-liability must be maintained and instead of weakening it, it should be strengthened.
- A criminal offense should be created when coercing workers, where a technical issue is reported in advance by a worker (knowledge).
- Legislation to limit the liability of Technology Workers and Contractors specifically. This essentially stunts the shifting of liability by corporations (including the practice of blame shifting onto technology staff, which is an abhorrent practice).
- Legislate stricter compliance and a (bi-partisan) registration body of all Cyber roles, not just Cyber Security, so that various aspects can be monitored including systematic abuse of the workforce. This should also require the reporting of wages, incentives, and employer offshore interests. This will naturally log experience also, limiting self-interests of; recruiters, consulting firms, labour hire.

- Legislate under one act, the explicit roles, responsibilities, rights, protections for all entities involved in Data/Technology/Privacy, including:
    - Governments, Federal and State
    - Corporations
    - Directors (inc. leaders)
    - Employees
    - Technology Workers (specifically)
    - Suppliers
    - Consumers / Citizens
        - Including Indirect consumers; minors, those recorded by others, people with carers.
- Examples of rights include what I have suggested in 2020 as, the **Right of Control**, over; privacy, security preferences, data; access, storage; with offenses created where organisations fail to provide such rights or impede upon them.
    - Standards-patterns may then be defined as a sub-section of that.
- Review stricter IP protections so that to limit incursion of IP treaties on Australia.
- Provide real incentives, with public disclosures, for corporations to assist in starting smaller technology organisations, from the prototype stage, where the start-up is also not directly or indirectly under the corporations control. Similar initiatives include ESVCLP, though the problem of no initial capital at the start, is a limitation for younger innovators. Examples that would benefit, include; a sole trader with a startup idea/solution/prototype, that can be built for the corporation, who is also the customer, where the corporation can be provided an incentive to fund the initial capital, along with the solution, without having any control over the startup.
- Mandatory disclosure and-also future updates to evidence law will be required. This can be used as mechanisms to collect evidence for the technology regulation.
    - Obviously, this means industry cannot be self-regulated and:
    - A bi-partisan legislated body that constantly pursues, and prosecutes, must be established.
    - Special care when updating evidence requirements is needed so that not to introduce new loopholes that can be exploited.
- Establish a bi-partisan legislated authority that can monitor service provider uptime, monitor business and customer complaints about service providers (including outages), then use this to detect issues and threats in real time, and finally compel the service provider for an immediate explanation.
- The existing frameworks and reforms are not sufficient to take us into the next decade. There is a real risk of harm.

What cyber security support, if any, should be provided to directors of small and medium companies?

- Small-and-medium (SME) businesses can be supported by SME technology providers. The decline of the SME technology providers over the last decade, assisted by government disinflationary policy, has resulted in exposure of small business to cyber issues. This can quickly and easily be undone by examining how to connect, and incentivise the use of, SME technology providers.

- This additionally creates a layer between small business and big-tech, giving small technology providers leverage and growth opportunities (if big-tech agreements are regulated also).
- This also assists in the creation of new Australian technologies and returns to the previous status quo.
- Such a strategy is timely. Nations across the world, including Singapore, are indicating that their home-grown technology sectors will be used to drive post-COVID recovery.

Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

- Awareness by senior business leaders is a non-issue. Ignorance of the law is no excuse. Current technology issues are widely understood anyway and have been under discussion for over a decade.

What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?

- Some Big-Tech providers formed their own black-internet systems by forcing client devices to recognise private top-level zone authorities. This practice went unreported for years.
- The following big tech behaviour is widely observed, yet went unchecked for years with many Cloud storage providers copying each-other's *glitch-by-design* (remains unchecked);
    - Actual Scenario: Any big tech provider is introducing a new cloud service that involves the storage of customer files. It then does the following to lock-in customer uptake;
        - Implements client software to connect and synchronise files to online storage,
        - Upon installation, the user or technician is not provided options on which files to sync,
        - The client software then continues to setup. This often happens without warning the user that it is collecting files across the device and force-uploading them. In some cases it would permanently destroy the original files (a bit like ransomware). In some cases the process cannot be stopped.
        - Take note that cloud providers have the capability to deny their customers access to their own files, e.g. should bills not be paid.
        - Take note big-tech has the capacity to ignore customers for complaints and support, without commercial repercussion.
        - When customers complain, they can be denied their complaint, or are asked to prove something that is impossible for the customer to prove – only to find out much later there was actually a problem.
        - Months/years later it would typically emerge that the behaviour is a "bug", and it is reported and "patched" (often) silently. It is unlikely that such behaviours are a technical glitch. As noted this onboarding process is by design, due to its lucrative nature.
        - After the "glitch" is removed, new behaviour to replace the previous is introduced, e.g. popup messages would be used to harass the user to upload files, even if it is a paid user. Sometimes the popups will be easy to accidently click on (as in the early worm viruses of the 90's).

        - Months or years later the business users would discover that the default settings for their file storage exposed the file-security. They would also discover that the power to create security gaps in file access is given to all its business users. Businesses discover that, to restrict access to the files; the business would have to pay for additional licenses and services, or perform highly complex product configurations (e.g. CLI configurations).
    - Actual Scenario: An existing major cloud storage provider has a session design that allows information to leak between organisations, where a user is a member of multiple organisations. This is a widely known issue and remains unreported.
    - The following big-tech legacy (pre-2011 internet governance) issues have been observed, yet remain unchecked:
        - Most of the big-tech cloud providers also provide authentication or identity-provider services as part of the package. Large numbers of corporations and SME business have spent considerable sums of money migrating to these systems under the impression that they are more reliable than traditional systems.
        - As we have already witnessed in recent years, these providers are not as reliable as traditional systems and are prone to:
            - Wide scale hacking.
            - Wide scale outages (affecting entire systems and economies).
            - Wide scale technical glitches that damage business digital assets. with no enforceable liability.
        - Offline mitigation solutions such as “hybrid” and “on-premise” are purposely being removed from product offerings, or not offered at all.
        - Physical “walls”, in the common law precedence sense of the terms, are purposely not being provided or offered in Cloud solutions.
    - Most concerningly, we are seeing an emergence of “pay for access control” and “pay for security” coming from big-tech. Where business and consumers are forced to pay additional subscription fees for basic security control and privacy, including access control to files.
    - Big-tech providers are increasingly employing lower skilled (offshore) staff for support, both in front facing and middle-senior tier support. This makes it impossible to resolve a technical issue, let alone report a cyber security issue. This, in some cases, has the effect of making certain the organisation is insulated from confirming a cyber security issue (a tactic).
        - Note; traditional internet governance standards required a direct line of communications to technical team leaders, that can be utilised by other third party technicians. This was considered a tenet of good governance for cyber security.
        - Note; some big-tech providers would also employ PR campaigns such as reward for bug schemes, though it is obvious that only a tiny portion of the applicable major security issues reported make it into those schemes.
- Big-tech providers are failing to provide adequate complaint avenues. For example;
    - A major technology supplier can stay under the radar by:
        - Supplying a non-functional complaints form, that may also be unmaintained, even if there is a court order by a regulator to have one.
        - Have a company established in Australia, but use an overseas entity for technical support, so that to limit liability, when:

    - It decides to deny a cyber security issue exists.
    - It decides not to repair the cyber security issue (costs transfer back to businesses and consumers).
    - Conscious awareness that Australian law can compel it to provide evidence.
- Big-tech can provide defective products as there is no national body that will recognise the views of subject matter experts, that is mutually recognised by experts. Customers are forced to pay lucrative amounts to fix problems. Dis-inflationary economic strategies, including labour hire and big-consulting, would then used to import cheaper and sometimes more expensive offshore workforce to maintain that status quo – insensibly this is done under regimes that falsely claim that there is a skills shortage.
- Labour-hire and dis-inflation of cyber workforce is also a highly recognised problem in all sectors. Industry enquiries are ongoing, and we would expect many security issues be raised. This includes issues of de-skilling the workforce so that to lower cost, while insensible claims are made that there is a lack of skills. In fact, the required Cyber skills are widely available at an appropriately higher cost. While lowering the cost of the workforce might sound good financially in the short term, this has a ripple effect, and most certainly it increases cyber security risk in the economy – and increases cost long term.
- Contrary to popular belief, there are no protections for business and consumer for the sale of dud (fake/useless/lemon) off-the-shelf software-based products, where the seller is offshore. Also, there is no authority that would investigate the technical workings of a product to prosecute. This is arguably a federal issue not a state issue.
- Telecommunications providers are capable of taking initiative or sharing initiatives to create preventative measures such as; alerts, monitoring, block lists, attack prevention; protecting the general public. This has not happened – organisations all act independently (often for profit), unless required to do so (rarely).
- Banks are not held to account for records keeping of access, and access controls (e.g. permitted to manually access and modify records, where the regulators have no technology enforcement capacity)
- Banks are de-banking technology businesses also (not just Blockchain or FinTech). Again regulators have no technology enforcement capacity.
- Banks providing inaccurate records. Again, regulators have no technology enforcement capacity.
- Banking delayed transactions and incorrect timestamps. Again, regulators have no technology enforcement capacity. This creates an entire network of delayed fees and denials of services across various industries including insurances. Further the regulators have no enforcement capacity to compel banks to produce records that prove record trails, such as system logs, in a timely manner. Regulators do not have the enforcement capacity to act against the flow-effects of systematic technology issues – after it has been reported. Regulators do not have the capacity to force providers to alter their offering so that not to disadvantage consumers under contract, where there is clearly delayed/altered/incorrectly-dated transactions due to systems design. This issue is not resolved by the recent instant transaction schemes.
- Bank statements are used as evidence in law despite deeply entrenched inaccuracy. Again, regulators have no technology enforcement capacity. The banks have full power over records. The regulators use the banks records as evidence only, leading to a chicken-and-the-egg evidence scenario.

- Banks not cleanly separating data and entities where related entities are regulated as separate entities. Again, regulators have no technology enforcement capacity.
- Banks charging exorbitant fees for technologies to customers. Practices that have been found to be illegal, though the practices continue. Various types of examples. Again, regulators have no technology enforcement capacity.
- Banks permitting business customers to withdraw consumer accounts without true authority, or where authority is withdrawn (as we have seen in direct debit, including direct debit fees). Where authority is withdrawn, denial of service to paid customers exists. Again, regulators have no technology enforcement capacity.
- Banks denial-of-service, or failure to provide electronic services, during outages – without compensation or penalty. Again, regulators have no technology enforcement capacity.
- Finger pointing in corporations, technology supply chains, regulators, and departments, has created a wild-wild-west in Cyber. Leaving consumers and citizens on their own to absorb the impact of the cyber issues presented to them. This includes issues with Digital ID's.
- There are hundreds of reported and unreported examples available. The list of gaps continues to grow daily, the only way to tackle them is by ensuring accountability and responsibility, by using strong penalty-based regimes. Such penalty-based regimes should not penalise technology workers but the ultimate decisions makers or people in power related to the issues that arise.
- Finally, and obviously, is ransomware. The wild-wild-west of Cyber has led us to be vulnerable. Ransomware, which is an important issue, is preventable, and it has been discussed thoroughly by many. The solution is not just virus or malware scanners. That would be a misconception (again lead by tick-the-box approaches). Ransomware has come ahead due to the laziness towards technology, by business leadership, and the lack of penalties. There is no doubt that technology workers have been raising this for nearly a decade. The issue is instead compounded with the use of online or centralised systems such as cloud systems.

END OF SUBMISSION